

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

PHISHME INC.,

Plaintiff,

v.

WOMBAT SECURITY TECHNOLOGIES,  
INC.,

Defendant.

C.A. No. \_\_\_\_

**JURY TRIAL DEMANDED**

**COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff PhishMe Inc. (“PhishMe”) brings this action for patent infringement against defendant Wombat Security Technologies, Inc. (“Wombat” or “Defendant”) and alleges as follows:

**NATURE OF THE ACTION**

1. PhishMe is the leading provider of phishing threat management for organizations concerned about human susceptibility and response to advanced targeted attacks. PhishMe’s intelligence-driven solutions empower employees to be an active line of defense and source of attack intelligence by enabling them to identify, report, and mitigate spear phishing, malware, and other cyberattacks.

2. PhishMe is built on technical innovation, borne of years of real-world experience in the cybersecurity trenches. PhishMe’s trailblazing technologies include PhishMe Simulator, PhishMe Reporter, and PhishMe Triage. PhishMe Simulator is a software-as-a-service (“SaaS”) platform that generates simulated phishing attack scenarios that organizations can use to increase their employees’ abilities to recognize and resist malicious phishing attempts. PhishMe Reporter

is a software plugin for email clients, such as Microsoft Outlook and Gmail, that provides an intuitive user-interface to enable an organization's employees to report suspicious emails to the organization's security team with the click of a button. PhishMe Triage, the first phishing-specific incident response platform, provides an organization's security team with real-time information about email-based attacks against the organization, allowing that team to collect and prioritize employee-reported threats.

3. PhishMe has protected its innovative solutions by obtaining numerous patents from the United States Patent and Trademark Office. In this action, PhishMe asserts United States Patent Nos. 9,591,017 ("the '017 Patent") and 9,674,221 ("the '221 Patent") (collectively, the "Asserted Patents"), both titled "Collaborative Phishing Attack Detection." The Asserted Patents claim methods and systems for identifying and processing email messages received at a remote computing device, such as a desktop computer or mobile phone, in connection with a simulated phishing email campaign. The '017 Patent covers aspects of PhishMe Simulator and PhishMe Reporter, while the '221 Patent covers aspects of these solutions as well as aspects of PhishMe Triage. In addition, PhishMe has asserted U.S. Patent No. 9,398,038 ("the '038 Patent"), which likewise is titled "Collaborative Phishing Attack Detection" and covers aspects of PhishMe Simulator and PhishMe Reporter, in C.A. No. 16-403-LPS, currently pending in the District of Delaware.

4. PhishMe's technical prowess has led to meteoric success in the cybersecurity field. From the public launch of PhishMe Simulator in 2008, PhishMe has grown to serve over a thousand customers worldwide, including many of the Fortune 100, Fortune 500, and Global 1000. PhishMe has achieved impressive growth, with an Annual Run Rate of approximately \$50 million, and having raised more than \$42 million in Series C funding.

5. Due to their success in the market and the strength of their innovations, PhishMe and its founders, Rohyt Belani and Aaron Higbee, have received numerous awards and honors. Among many others, SC Magazine bestowed PhishMe with the award for Best IT Security-Related Training Program and selected PhishMe as Hall of Fame Innovators in 2016, Deloitte included PhishMe in its Technology Fast500 Fastest Growing Companies list in 2015, and Washingtonian magazine named PhishMe's founders, Rohyt Belani and Aaron Higbee, as 2017 Tech Titans. In addition, Gartner has recognized PhishMe as a "leader" in its Magic Quadrant for Security Awareness Computer Based Training.

6. Following this success, PhishMe's rivals have attempted to imitate its innovative solutions. At issue here is PhishMe's direct competitor, Wombat Security Technologies, Inc., which has trailed PhishMe in both innovation and success. After PhishMe released PhishMe Reporter in 2013 and subsequently enjoyed significant growth and recognition in the market, Wombat found itself in a decidedly inferior competitive position. On information and belief, Wombat chose to respond to this deficit not by innovating, but by adopting a culture of copying. Wombat responded to the success of PhishMe Reporter with an imitation, called PhishAlarm. After PhishMe repeated its success by releasing PhishMe Triage in 2015, Wombat responded by releasing another imitation, called PhishAlarm Analyzer, one year later.

7. Wombat extended its culture of copying by acquiring ThreatSim, a competing phishing simulation solution, in October 2015 from Stratum Security. On information and belief, Stratum sought to piggyback on PhishMe's success, leading it to produce its own imitations: ThreatSim and its associated email client plugin, ThreatSim for Outlook. On information and belief, Wombat acquired ThreatSim at least in part so that it could better compete with PhishMe.

Following the October 2015 acquisition, Wombat has integrated ThreatSim into its product offerings and, on information and belief, has continued to support ThreatSim for Outlook.

8. As alleged in detail below, Wombat is infringing PhishMe's '017 and '221 Patents directly by making, using, offering for sale, or selling software solutions, including PhishAlarm, PhishAlarm Analyzer, ThreatSim, ThreatSim for Outlook, and PhishGuru, and indirectly by inducing or contributing to the infringement of those patents by others, including Wombat's customers. PhishMe has filed this action to put an end to Wombat's illegal acts and to obtain fair compensation for Wombat's infringement.

### **THE PARTIES**

9. PhishMe is a Delaware corporation, with its principal place of business located at 1608 Village Market Boulevard, SE # 200, Leesburg, Virginia 20175.

10. Wombat is a Delaware corporation, with its principal place of business located at 3030 Penn Avenue, Suite 200, Pittsburgh, Pennsylvania 15201.

### **JURISDICTION AND VENUE**

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a). The Court has personal jurisdiction over Wombat because Wombat is a Delaware corporation established and existing under the laws of Delaware. Moreover, Wombat has admitted that the exercise of personal jurisdiction over it is proper in this judicial District.<sup>1</sup>

12. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b) and (c) and 1400(b) because Wombat resides in this judicial District. Wombat also has admitted that venue is proper in this judicial District.<sup>2</sup>

---

<sup>1</sup> Wombat's Answer & Counterclaims, D.I. No. 18 ¶ 5, *PhishMe Inc. v. Wombat Security Technologies, Inc.*, C.A. No. 16-403-LPS-CJB (D. Del. Sept. 20, 2016).

<sup>2</sup> *Id.* ¶ 6.

### **RELATED LITIGATION**

13. PhishMe is currently asserting the '038 Patent against Wombat in the action titled *PhishMe Inc. v. Wombat Security Technologies, Inc.*, C.A. No. 16-403-LPS, pending in this Court. The Asserted Patents are related to the '038 Patent.

### **BACKGROUND**

#### **A. Phishing Poses a Significant Internet Threat to Organizations' Computing Systems**

14. Computer systems have become a vital element of every organization. In particular, computer systems increasingly are used to store enormous amounts of highly sensitive information, including business information, intellectual property, and governmental secrets.

15. As organizations' dependence on their computer systems has risen and as these systems are largely interconnected, the risks to those systems' integrity also have increased. One of the greatest threats to computer systems' integrity in the Internet age is known as "phishing." Phishing is a form of cyberattack in which a fraudulent email is disguised as a legitimate communication. A phishing email typically attempts to trick the recipient into responding, such as by clicking a link to a fraudulent webpage, downloading a malicious attachment, or directly providing sensitive information. A successful phishing attack can compromise the recipient's computer system, as well as the computer system of the recipient's organization, such as by giving the cyber-attacker a foothold in the organization's computer network or by providing access to vital information, such as proprietary or personal data. A recent report indicated that the heads of Goldman Sachs, Citigroup, Barclays, and the Bank of England have fallen victim to phishing attacks.<sup>3</sup>

---

<sup>3</sup> Anjuli Davies and Olivia Oran, *U.S. bank bosses succumb to email hoaxes*, Reuters, June 12, 2017, available at <https://uk.reuters.com/article/us-banks-email-idUKKBN1931SU>.

16. The impact of such phishing attacks is severe: they claim millions of victims and have caused billions of dollars in damage.<sup>4</sup> The Federal Bureau of Investigation has estimated the losses from Business E-mail Compromise attacks, which can be facilitated via phishing, have caused losses totaling more than \$5.3 billion worldwide.<sup>5</sup> The Department of Justice recently announced criminal charges against an individual who tricked two multinational internet companies into wiring more than \$100 million into overseas bank accounts by sending phishing emails purporting to be from employees of a company that regularly conducted business with the victim companies.<sup>6</sup>

17. In addition, cyber-criminals often use phishing to initiate ransomware attacks, in which malware prevents or limits access to a computer system until the victim pays a ransom.<sup>7</sup> A ransomware attack against Hollywood Presbyterian Medical Center in 2016 disabled access to the hospital's electronic medical records system and other computer systems until the hospital paid a ransom equaling \$17,000.<sup>8</sup>

18. Phishing attacks have been waged against not only businesses' computer systems, but also against those of governmental and public service organizations, such as hospitals,

---

<sup>4</sup> Ammar Almomani, et al., *A Survey of Phishing Email Filtering Techniques*, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol. 15, pp. 2070-2090 (2013).

<sup>5</sup> Public Serv. Announcement, Business E-Mail Compromise, E-Mail Account Compromise, The 5 Billion Dollar Scam, Fed. Bureau of Investigation, May 4, 2017, <https://www.ic3.gov/media/2017/170504.aspx>.

<sup>6</sup> Press Release, United States Dep't of Justice, Lithuanian Man Arrested For Theft Of Over \$100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies (Mar. 21, 2017), <https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme>.

<sup>7</sup> Fed. Bureau of Investigation, Ransomware Information Sheet, <http://www.americanbar.org/content/dam/aba/administrative/cyberalert/ransomware.authcheckdam.pdf>.

<sup>8</sup> See Sean Gallagher, *Hospital pays \$17k for ransomware crypto key*, Ars Technica, Feb. 18, 2016, <http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/>.

schools, and police departments.<sup>9</sup> A phishing attack led to the hack of the Democratic National Committee during the lead-up to the 2016 elections.<sup>10</sup> A separate phishing attack led to the hack of a U.S. voting systems manufacturer shortly before the 2016 elections.<sup>11</sup> And a 2015 phishing attack against the United States Office of Personnel Management has been called “the biggest government hack ever.”<sup>12</sup>

19. Phishing attacks also pose a significant threat to national security. In 2012, Defense Secretary Leon Panetta warned of a possible “cyber-Pearl Harbor” and noted that the United States has become increasingly vulnerable to foreign computer hackers who could dismantle the nation’s power grid, transportation system, financial networks, and government.<sup>13</sup> According to a March 2017 report from the Office of Management and Budget, more than 30,000 “cyber incidents” in 2016 affected Federal agencies, including thousands of email

---

<sup>9</sup> See, e.g., Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, Wired, Mar. 30, 2016, available at <https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/>; Fed. Bureau of Investigation, *Incidents of Ransomware on the Rise*, Apr. 29, 2016, <https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise>.

<sup>10</sup> See Eric Lipton, et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. Times, Dec. 13, 2016, available at [https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?\\_r=0](https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0).

<sup>11</sup> See David Smith and Jon Swaine, *Russian agents hacked US voting system manufacturer before US election – report*, The Guardian, June 5, 2017, available at <https://www.theguardian.com/technology/2017/jun/05/russia-us-election-hack-voting-system-nsa-report>.)

<sup>12</sup> See Sean Gallagher, *Why the “biggest government hack ever” got past the feds*, Ars Technica, June 8, 2015, <http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/>.

<sup>13</sup> Elisabeth Bumiller and Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times, Oct. 11, 2012, available at [http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?\\_r=0](http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0).

phishing attacks that led to the “compromise of information or system functionality” to the Department of Homeland Security’s U.S. Computer Emergency Readiness Team.<sup>14</sup>

**B. PhishMe’s Patented Technology Protects Organizations and Improves Their Computing Systems’ Security, Integrity, and Functionality**

20. PhishMe is a pioneering company in assessing, combating, and preventing phishing and other cyberattacks. Since it launched its cybersecurity service publicly in 2008, PhishMe has become the leading provider of threat management for organizations concerned about human susceptibility to advanced targeted attacks. PhishMe’s success in helping to secure its customers’ computer systems against cyberattacks owes to its innovative technology, which utilizes user-generated intelligence to defend against phishing threats in a timely manner.

21. PhishMe’s computer technology includes its PhishMe Simulator™ product for generating simulated phishing emails. PhishMe Simulator allows organizations to generate simulated phishing emails and send the simulated phishing emails to users of the organization. If a user of the organization falls victim to the simulated phishing email by, for example, opening an embedded link, the user is provided with immediate feedback. The feedback helps to build user awareness to phishing attacks, reduces their susceptibility to fall for real phishing attacks in the future, and encourages users to rapidly report suspicious emails to their information technology departments. PhishMe Simulator also includes a Dashboard display for collecting and sharing metrics about employee responses to simulated phishing emails and trends demonstrating improvement in employee recognition of those messages.

---

<sup>14</sup> Nafeesa Syeed, *Cybersecurity Gaps Existing Federal Agencies, White House Report Finds*, Government Technology, Mar. 13, 2017, <http://www.govtech.com/security/Cybersecurity-Gaps-Exist-in-Federal-Agencies-White-House-Report-Finds.html>; Exec. Office of the President of the United States, Federal Information Security Modernization Act of 2014, Annual Report to Congress, Fiscal Year 2016, [https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy\\_2016\\_fisma\\_report%20to\\_congress\\_official\\_release\\_march\\_10\\_2017.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf).

22. Another key element of PhishMe's computer technology is PhishMe Reporter®, a software plugin that improves upon existing phishing prevention systems by adding a user-interface that allows computer users to report suspicious emails to internal security teams or computer systems in a timely manner. The suspicious emails that users report could be simulated phishing emails generated by PhishMe Simulator and sent as part of a training campaign or potentially real phishing emails sent as part of an attack. PhishMe Reporter enhances phishing detection and response systems by automatically distinguishing between simulated and potentially real phishing emails, so that reports of possibly malicious emails are delivered to appropriate security operations and incident response teams. This saves significant computing resources and accelerates the detection of actual threats, and thus improves the overall security, integrity, and functionality of the organization's computing systems. PhishMe Reporter also gives end users immediate feedback when they report simulated phishing emails to reinforce and encourage their positive behavior. This allows organizations to leverage human intelligence to identify and detect phishing attacks, thereby preventing damage to computing systems and large-scale data breaches.

23. PhishMe's technology also includes PhishMe Triage™, which automatically prioritizes reported emails by threat level. PhishMe Triage focuses customer incident response teams on the reported emails that are most likely to be malicious and eliminates time spent chasing false positives—*i.e.*, emails reported by users that are not malicious. This technology also assists incident response teams in their analyses of such reported emails and in creating rules and playbooks to interact with other defensive systems to block the identified emails sent with malicious intent.

24. PhishMe has obtained numerous patents on its innovative cybersecurity technologies. At the heart of this action are the '017 and '221 Patents, both titled "Collaborative Phishing Attack Detection," and issued to Aaron Higbee, Rohyt Belani, and Scott Greaux on March 7 and June 6, 2017, respectively. The Asserted Patents are related and have a common specification, as the '221 Patent issued from a continuation of the application that led to the '017 Patent. PhishMe owns all right, title, and interest in and to the Asserted Patents, copies of which are attached as Exhibits A and B, respectively.

25. The Asserted Patents cover systems and methods for generating simulated phishing attacks, detecting whether an incoming email is a simulated or potential phishing attack, and training users to correctly identify and report phishing attacks. Their common specification discusses prior art solutions to combating phishing attacks, such as "computer programs designed to detect and block phishing emails."<sup>15</sup> The specification explains that these prior art solutions are insufficient because they cannot adapt to the dynamic nature of phishing attacks, as "phishing attack methods are constantly being modified by attackers to evade such forms of detection."<sup>16</sup>

26. The Asserted Patents' claimed inventions improve on these prior art technologies. The claimed inventions allow one to generate a simulated phishing email with at least one embedded hyperlink and to transmit the simulated phishing email to a remote computing device. They include a plugin at a remote computing device that allows a user to report an email as a potential phishing attack. They use the email's header and stored or identifying information to identify the reported email as either a simulated phishing email or a potentially malicious phishing attack. If the former, the user receives feedback confirming that the identified email

---

<sup>15</sup> '017 Patent at 1:51-52.

<sup>16</sup> *Id.* at 1:46-48.

was a simulated phishing email. If the latter, the patented inventions send the potentially malicious phishing attack for analysis or detection of whether it is an actual phishing attack. In addition, the claimed inventions record data indicating that the reported email has been identified as a simulated phishing attack or as a potentially malicious phishing attack. The claimed inventions provide electronic training to the user if he or she clicks on a simulated phishing email's embedded hyperlink. Finally, the '221 Patent's claimed invention computes a likelihood that a potentially malicious phishing attack reported by a user is an actual phishing attack based on one or more attributes of the reported email.

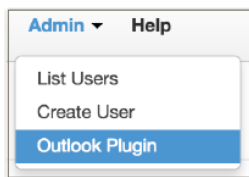
**C. Wombat's Products, Software, and Services**

27. Wombat is a provider of cybersecurity products, including phishing awareness technology. Wombat markets, makes, sells, offers for sale, and uses its "Security Education Platform," an integrated SaaS-based platform through which Wombat provides various products, software, and services, including ThreatSim, PhishAlarm, and PhishAlarm Analyzer. Wombat's cybersecurity products also include ThreatSim for Outlook and PhishGuru, which Wombat has marketed, sold, and offered for sale and continues to use and support. Wombat has made, marketed, sold, offered for sale, and supported ThreatSim, PhishAlarm, PhishAlarm Analyzer, ThreatSim for Outlook, PhishGuru, and other components of its Security Education Platform (collectively, "the Accused Products") in the United States. In addition, Wombat also provides "managed services," through which it uses the Accused Products in the United States to provide simulated phishing training to its customers.

28. As discussed above, in October 2015, Wombat acquired ThreatSim and its accompanying email client plugin, ThreatSim for Outlook, from Stratum Security. Wombat subsequently incorporated ThreatSim into its Security Education Platform and, on information and belief, has continued to support ThreatSim for Outlook. Like PhishMe's patented inventions,

ThreatSim for Outlook includes a user interface allowing the user to report a suspicious email as a possible phishing attack:

Within the ThreatSim portal click the Admin menu and select Outlook Plugin:



Download the ThreatSim for Outlook installer:

Outlook Plugin Configuration				
CATEGORIES	Download	File	Version	SHA Checksum
Installation Keys				
Configure Plugin				
Download Installer		Local Installer	1.0.4	1738576e45e01f55ea8b73b6b7029b49c4c8de7
		Citrix Installer	1.0.4	a35db84ca67a558ea7fa1a1d5eed3d53ee9ecf

### ThreatSim® for Outlook Administrator Guide

(available at <https://www.wombatsecurity.com/security-education/simulated-phishing-attacks>)

29. Also like PhishMe's patented inventions, ThreatSim for Outlook uses the email header and stored or identifying information to distinguish between a simulated phishing attack and a potentially malicious phishing attack:

All ThreatSim emails contain a custom SMTP header that looks like this:

```
X-ThreatSim-Header: http://threatsim.com/speartraining?id=765fa3
X-ThreatSim-ID: 765fa3
```

The X-ThreatSim-ID allows ThreatSim to identify which campaign and which user reported the email.

When the user clicks on the ThreatSim for Outlook button, Outlook will connect to our API at <https://outlook.threatsim.com> and send us the X-ThreatSim-ID. We then correlate the ID to the campaign and the target user, and mark the user as "Reported" within ThreatSim

If the X-ThreatSim-ID header is **not** found within the email, ThreatSim for Outlook forwards the email to the email address configured within your settings. The email is sent as a .eml attachment using the user's Outlook and is NOT sent to ThreatSim.

### ThreatSim® for Outlook Administrator Guide

30. Additionally, like PhishMe's patented inventions, if the identified email is a simulated phishing attack, ThreatSim for Outlook provides user feedback. If not, the identified email is forwarded on to an identified email address for further analysis:

**Customize the message you want displayed when the email IS a ThreatSim message:**

Correct Report Alert	Congratulations! That was a simulated phishing email sent by [ENTER YOUR ORGANIZATION'S NAME] It is users like you that help keep us secure. Keep up the good work!
----------------------	---

**Customize the message you want displayed when the email IS NOT a ThreatSim message:**

Non-ThreatSim Report Alert	Thank you for reporting this suspicious email to the [ENTER YOUR ORGANIZATION'S NAME] . It is users like you that help keep us secure!
----------------------------	--

### **ThreatSim® for Outlook Administrator Guide**

31. Also like PhishMe's patented inventions, if a user falls for a mock attack by clicking on a simulated phishing email, ThreatSim automatically presents a user with electronic training on how to distinguish malicious and benign emails:

Our ThreatSim® attack simulation product is an excellent option if you are looking to deliver a phishing-focused security awareness training program. The ThreatSim mock attack system allows you to deliver simulated phishing emails with embedded Teachable Moments, which display targeted "just-in-time teaching" messages to individuals who fall for a simulated attack.

- Automatically presents any employee who falls for a mock attack with a Teachable Moment (see below), which explains the situation and provides practical guidance and tips for future reference.

### **ThreatSim Simulated Phishing Attacks**

(available at <https://www.wombatsecurity.com/security-education/simulated-phishing-attacks>)

32. On information and belief, Wombat's pre-acquisition products function similarly to ThreatSim and ThreatSim for Outlook. Prior to incorporating ThreatSim into its Security Education Platform, Wombat made, used, offered for sale, sold, and supported PhishGuru, a SaaS-based solution that, like ThreatSim, is used to generate simulated phishing attacks. And like PhishMe's patented inventions, if a user falls for a PhishGuru mock attack by clicking on a simulated phishing email, PhishGuru automatically presents a user with training on how to distinguish malicious and benign emails:

- Automatically presents any employee who falls for a mock attack with a Teachable Moment (see below), which explains the situation and provides practical guidance and tips for future reference.

#### **PhishGuru Simulated Phishing Attacks**

(available at <https://www.wombatsecurity.com/security-education/phishguru-simulated-phishing-attacks>)

33. As discussed above, Wombat also developed PhishAlarm, an email client plugin used in conjunction with PhishGuru or, following the acquisition, ThreatSim to allow an organization's employees to report suspicious messages:

#### **PHISHALARM: ONE-CLICK REPORTING OF SUSPECTED PHISHING EMAILS**



Our PhishAlarm email reporting button gives your users the ability to report suspected phishing emails to your security and incident response teams with a single mouse click. As a component of our ThreatSim® simulated attack assessments, PhishAlarm allows users to draw on their knowledge and use learned behaviors to stop social engineers and hackers in their tracks.

#### **PhishAlarm Email Reporting Button and Security Awareness Materials**

(available at <https://www.wombatsecurity.com/security-education/reinforce>)

- Includes our PhishAlarm® one-click email reporting (/security-education/reinforce) tool. This email client add-in allows employees to report suspicious messages to your security and incident response teams with a single mouse click.

#### **ThreatSim Simulated Phishing Attacks**

34. Wombat also markets and sells PhishAlarm Analyzer. Like PhishMe's patented inventions, PhishAlarm Analyzer automatically prioritizes reported emails by threat potential, "allowing your security teams to focus their time and attention on the most imminent and dangerous threats to your network." PhishAlarm Analyzer examines attributes and content of reported emails to determine the likelihood that a reported email is an actual phishing attack. (<https://www.wombatsecurity.com/security-education/phishalarm-and-analyzer>)

**COUNT I – PATENT INFRINGEMENT**  
**(U.S. Patent No. 9,591,017)**

35. PhishMe incorporates by reference and re-alleges Paragraphs 1–34 above as though fully restated herein.

36. Wombat has directly infringed the '017 Patent by making, using, selling, and offering for sale in the United States, without license or authority, products, software, and services that infringe, literally or under the doctrine of equivalents, one or more of the claims of the '017 Patent in violation of 35 U.S.C. § 271(a).

37. In addition, Wombat knowingly and intentionally has induced infringement of the '017 Patent under 35 U.S.C. § 271(b) by actively encouraging others to make, use, sell, and offer for sale in the United States, without license or authority, products, software, and services that infringe, literally or under the doctrine of equivalents, one or more of the claims of the '017 Patent. For example, Wombat has instructed and encouraged its customers to use its infringing products and software to perform the claimed methods of the '017 Patent, including through the following: (i) providing instructions and services to end users and customers of Wombat's products for using the products in their customary way; (ii) providing to third parties the products and software and related services that may be required for or associated with

infringement of the '017 Patent; (iii) selling and offering to sell Wombat's infringing products in the United States; and (iv) promoting the infringing products on Wombat's website. On information and belief, Wombat has undertaken the above actions with knowledge that the induced acts infringe one or more claims of the '017 Patent, or Wombat subjectively believes that there is a high likelihood that the induced acts infringe the '017 Patent and it has taken deliberate steps to avoid learning that the induced acts do infringe the '017 Patent.

38. Further, Wombat has contributed to the infringement of the '017 Patent under 35 U.S.C. § 271(c) by selling and offering for sale, without license or authority, the infringing products and software in the United States, knowing that such products and software are especially made or adapted for use in infringement of the '017 Patent, are not a staple article or commodity of commerce suitable for any substantial non-infringing use, and that others, such as Wombat's customers and end-users, use such products and software to infringe the '017 Patent.

39. On information and belief, Wombat monitors PhishMe's portfolio of pending patent applications and thus has had knowledge of the '017 Patent and the infringing nature of its activities since the '017 Patent issued on March 7, 2017. As evidence of this monitoring, Wombat identified the '017 Patent application (serial no. 15/138,188) in its unsuccessful January 3, 2017 Petition for Post-Grant Review (PGR) of PhishMe's '038 Patent before the Patent Trial and Appeal Board. Furthermore, Wombat has known of PhishMe's cybersecurity inventions, including those described in the '017 Patent, since at least August 21, 2015, when Wombat cited a related patent, U.S. Patent No. 8,719,940, as prior art during prosecution of its own patent application. Moreover, Wombat has known of the '017 Patent at least as of the filing of this Complaint. Despite knowing that it is infringing the '017 Patent, Wombat has continued to make, use, sell, and offer for sale its infringing products, software, and services and to actively

encourage others to use its infringing products, software, and services to perform the '017 Patent's claimed methods.

40. PhishMe has been and continues to be damaged by Wombat's infringement of the '017 Patent in an amount to be determined and subject to proof at trial. In addition, Wombat's infringement of the '017 Patent has irreparably harmed PhishMe. Among other things, Wombat is competing against PhishMe by using PhishMe's own patented inventions.

**COUNT II – PATENT INFRINGEMENT**  
**(U.S. Patent No. 9,674,221)**

41. PhishMe incorporates by reference and re-alleges Paragraphs 1–40 above as though fully restated herein.

42. Wombat has directly infringed the '221 Patent by making, using, selling, and offering for sale in the United States, without license or authority, products, software, and services that infringe, literally or under the doctrine of equivalents, one or more of the claims of the '221 Patent in violation of 35 U.S.C. § 271(a).

43. In addition, Wombat knowingly and intentionally has induced infringement of the '221 Patent under 35 U.S.C. § 271(b) by actively encouraging others to make, use, sell, and offer for sale in the United States, without license or authority, products, software, and services that infringe, literally or under the doctrine of equivalents, one or more of the claims of the '221 Patent. For example, Wombat has instructed and encouraged its customers to use its infringing products and software to perform the claimed methods of the '221 Patent, including through the following: (i) providing instructions and services to end users and customers of Wombat's products for using the products in their customary way; (ii) providing to third parties the products and software and related services that may be required for or associated with infringement of the '221 Patent; (iii) selling and offering to sell Wombat's infringing products in

the United States; and (iv) promoting the infringing products on Wombat's website. On information and belief, Wombat has undertaken the above actions with knowledge that the induced acts infringe one or more claims of the '221 Patent, or Wombat subjectively believes that there is a high likelihood that the induced acts infringe the '221 Patent and it has taken deliberate steps to avoid learning that the induced acts do infringe the '221 Patent.

44. Further, Wombat has contributed to the infringement of the '221 Patent under 35 U.S.C. § 271(c) by selling and offering for sale, without license or authority, its infringing products and software in the United States, knowing that such products and software are especially made or adapted for use in infringement of the '221 Patent, are not a staple article or commodity of commerce suitable for any substantial non-infringing use, and that others, such as Wombat's customers and end-users, use such products and software to infringe the '221 Patent.

45. On information and belief, Wombat monitors PhishMe's portfolio of patents and pending patent applications and thus has known of the '221 Patent and the infringing nature of its activities since that patent issued on June 6, 2017. Furthermore, Wombat has known of PhishMe's cybersecurity inventions, including those described in the '221 Patent, since at least August 21, 2015, when Wombat cited a related patent, U.S. Patent No. 8,719,940, as prior art during prosecution of its own patent application. Further, Wombat has known of the '221 Patent at least as of the filing of this Complaint. Despite knowing that it is infringing the '221 Patent, Wombat has continued to make, use, sell, and offer for sale its infringing products, software, and services and to actively encourage others to use its infringing products, software, and services to perform the '221 Patent's claimed methods.

46. PhishMe has been and continues to be damaged by Wombat's infringement of the '221 Patent in an amount to be determined and subject to proof at trial. In addition,

Wombat's infringement of the '221 Patent has irreparably harmed PhishMe. Among other things, Wombat is competing against PhishMe by using PhishMe's own patented inventions.

**JURY DEMAND**

47. PhishMe demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to Fed. R. Civ. P. 38 and D. Del. LR 38.1.

**PRAYER FOR RELIEF**

WHEREFORE, PhishMe respectfully requests that this Court enter judgment in its favor as follows:

- A. Declare that Wombat has infringed the Asserted Patents, either literally or under the doctrine of equivalents;
- B. Declare that Wombat has induced infringement of the Asserted Patents;
- C. Declare that Wombat has contributed to the infringement of the Asserted Patents;
- D. Award PhishMe past and future damages, together with prejudgment and post-judgment interest, to compensate for Wombat's infringement of the Asserted Patents in accordance with 35 U.S.C. § 284;
- E. Declare that this case is exceptional under 35 U.S.C. § 285;
- F. Award PhishMe its costs and attorneys' fees under 35 U.S.C. § 285;
- G. Issue an injunction barring Wombat and its officers, directors, agents, employees, affiliates, attorneys, and all others acting in privity or in concert with it, and its parents, subsidiaries, divisions, successors, and assigns, from further acts of infringement of the Asserted Patents; and
- H. Grant PhishMe such other and further relief as the case may require and the Court may deem just and proper under the circumstances.

OF COUNSEL:

MORRISON & FOERSTER LLP  
Hector G. Gallegos  
Mehran Arjomand  
707 Wilshire Boulevard  
Los Angeles, California 90017-3543  
(213) 892-5200  
hgallegos@mofo.com  
marjomand@mofo.com

Joshua A. Hartman  
Fahd H. Patel  
2000 Pennsylvania Ave., NW  
Washington, DC 20006-1888  
(202) 887-1500  
jhartman@mofo.com  
fpatel@mofo.com

Dated: June 16, 2017

01:22034904.1

YOUNG CONAWAY STARGATT & TAYLOR, LLP



Anne Shea Gaza (No. 4093)  
Samantha Wilson (No. 5816)  
Rodney Square  
1000 North King Street  
Wilmington, DE 19801  
(302) 571-6600  
agaza@ycst.com  
swilson@ycst.com

*Attorneys for Plaintiff PhishMe, Inc.*